Secure and Efficient Cluster Selection Mechanism Using Wimax

Vinni Kaur[1], Amanpreet Kaur[2], Arvind Pathak[3]
Electronics and Communication Engineering[1,2,3]
Lingaya's University[1, 2, 3]
Faridabad (NCR), India[1, 2, 3]

Abstract— **WiMAX technology is a telecommunications technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoint links. As the size of a Wireless Network is much vast because of this the network containing number of base station and mobile station is divided in terms of clusters. Each cluster having a cluster head or the base station the controls all nodes of the network. A WiMAX can have a node with the mobility. The problem begins when a node moves from the cluster and when outside the range of Cluster head. In such case the control of that node shifted to other Cluster Head. This process is called head off machism. The resulted system is the scheme to elect the best cluster head for this node respective to the security and efficiently. In this work we have do some basic parameter changes i.e. number of packet transfer, last packet time, bit rate, byte rate, packet lost, and packet delay time while performing the selection of base station. The analysis is performed for having the effective throughput and the delay. Now we use the public key cryptography, RSA to implement and achieve the secure handoff. The analytical results shows that the use of WiMAX in handover during communication gives better efficiency.**

Keywords--WiMAX; Handoff; Packets; cryptography; secure and efficient.

I. INTRODUCTION

WiMAX is one of the hottest broadband wireless technologies around today. These systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. When we work with a large WiMAX network with n number of clusters and the nodes over the network having the mobility in itself. A node moves from one cluster area to other, in some case it is possible that more than one cluster head claim the control on that node. In such case we have to decide which CH will be selected to take the control of communication for that network. The node selection must be reliable, secure and efficient. The proposed approach is the work in the same direction such that a secure handover will be performed. A secure and efficient handover will result the efficient transmission over the network.

II. WIMAX

WiMAX is a revolutionary wireless technology that has a rich set of technological improvements compare to the other broadband access technology. WiMAX stands for Worldwide Interoperability for Microwave Access. WiMAX technology is a telecommunications technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoint links.

The WiMAX technology offers around 72 Mega Bits per second without any need for the cable infrastructure. WiMAX technology is based on Standard that is IEEE 802.16, it usually also called as Broadband Wireless Access. WiMAX Forum created the name for WiMAX technology that was formed in Mid June 2001 to encourage compliance and interoperability of the WiMAX IEEE 802.16 standard. WiMAX technology is actually based on the standards that making the possibility to delivery last mile broadband access as a substitute to conventional cable and DSL lines[3]. The set of features of WiMAX are listed below:

a) OFDM based physical layer
b) Quality of service:
c) Flexible architecture
d) TDD and FDD support:.
e) Adaptive modulation and coding
f) High data rate:
g) Mobility support: Strong Security:.

A. WiMAX Architecture and Other Technical Facts

WiMAX is the next generation broadband wireless technology which not only offers the greater flexibility but also covers longer distances. Its technological advances significantly reduce the service cost compare to the other broadband technology like DSL, ultra wideband (UWB) family of standards and Wi-Fi. This subsection describes the architecture of WiMAX and its technical features [4].

Fig. 1 shows the management reference model for BWA (Broadband Wireless Access) networks. This consists of a Network Management System (NMS), some nodes, and a database. BS and SS managed nodes collect and store the managed objects in an 802.16 MIB format. Managed objects are made available to NMS using the Simple Network Management Protocol (SNMP).

When a customer subscribes to the WiMAX service, the service provider asks the customer for the service flow information. This would include number of UL / DL connections with the data rates and QoS parameters. The customer also needs to tell the kind of applications that he proposes to run.

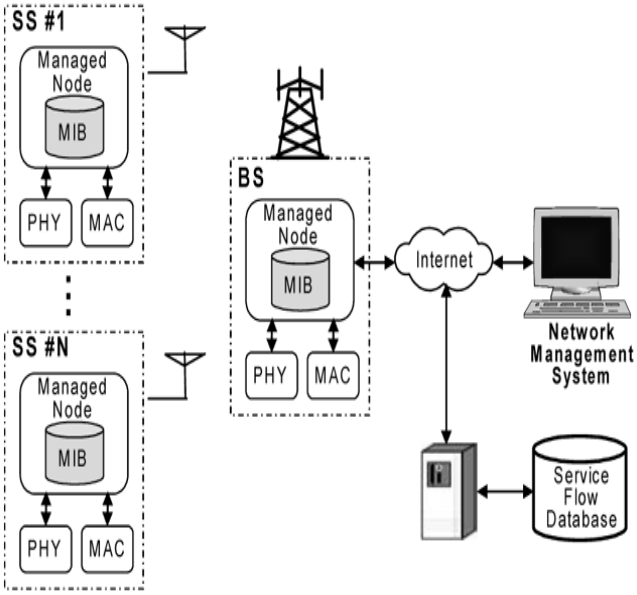

Figure 1. *WiMAX Management Information Base*

B. WiMAX Connectivity

Depending on the frequency range WiMAX can provide two types of Wireless services, Line of sight (LOS) and Non line of sight (NLOS)].

Line of Sight (LOS): LOS operates in higher frequencies between 10-66 GHz. This frequency range is called millimeter bands. Since line of sight uses higher frequencies, it can provide higher bandwidth with less interference. It's coverage area also huge. Theoretically it is 30 mile radius. For LOS there should be direct contact between the WiMAX tower and the dish antenna from the customer sight which could be placed in the rooftop or a pole. In this way subscriber can get great data capacity.

Non Line of Sight (NLOS): NLOS uses lower frequencies between 2 GHz to 11 GHz. This lower frequency range is called centimeter band. The advantage of these lower frequencies is, it can bend or diffract around obstacles. This advantage helps the multipoint communication, so more customers can get the services from a single tower which reduces the service cost also. In this way WiMAX enabled computers can get full speed internet services within the coverage area but the coverage is lower than the line of sight communication. Usually it is 4 to 6 mi radius which is similar to a cell phone coverage area.

As the size of a Wireless Network is much vast because of this the complete network is divided in terms of clusters. Each cluster having a cluster head or the base station the controls all nodes of the network. A Wimax can have a node with the mobility. The problem begins when a node moves from the cluster and when outside the range of Cluster head. In such case the control of that node shifted to other Cluster Head. This process is called head off machismo. The proposed system is the scheme to elect the best cluster head for this node respective to the security and efficiently.

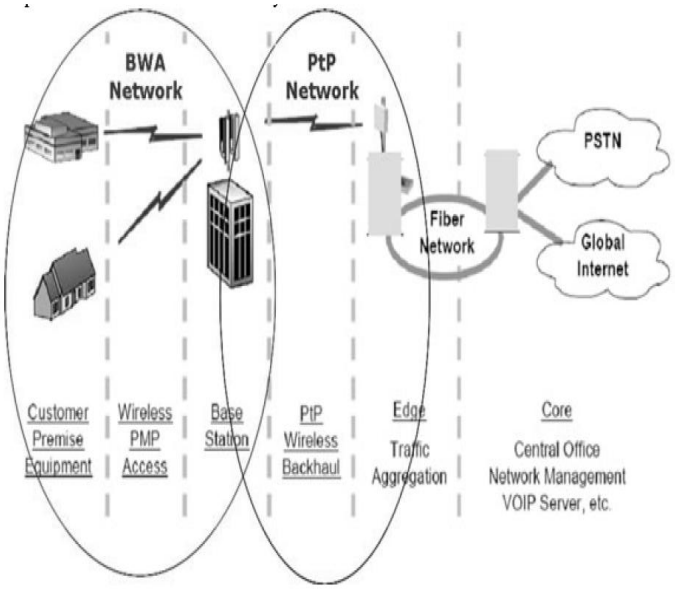

Figure 2. WiMAX Connectivity

III. HANDOVER

Three types of handoffs are defined by the IEEE 802.16e, hard handoff (HHO), Macro Diversity Handoff (MDHO) and Fast Base Station Switching (FBSS). Out of these three handoff types, HHO is mandatory and the other two are optional. Types of handoff:

Hard Handoff (HHO): Mobile stations maintaining the communication with a single BS at any given time. So depending on the signal strength, MS breaks the communication with lower signal strength BS and establish the connection with the higher signal strength BS during its travel between different BS.

Macro Diversity Handover: MDHO is similar to a soft handover in nature where within a diversity set, MS maintains communication with multiple BS. A set of BS which are treated as diversity set are responsible for handoff procedure. In case of downlink within MDHO, a mobile station receives data from several base stations; as a result diversity could be combined within the mobile station. In uplink, MS transmits signal to several BS. The Selection diversity process takes place in these BS's. Neighboring BS are those which communicates with the MS and other base station with weaker signal.

Fast Base Station Switching: FBSS, mobile station monitors all BS and selects one BS as an Anchor BS where it registered and passing all the uplink and downlink data. Synchronization and monitoring control information also performing through this base station.

A. Efficient Handover

The proposed handover scheme will evaluate the maximum effective capacity and the idle capacity of the base station for any point of time in the network. The triggering will be performed based on some decision factor. Base station having the more effective capacity will be elected for the next base station after handover. The proposed system will provide a reliable and energy efficient hand over. The steps involved in the algorithm are given here:

Let the communication is being performed between 2 nodes present in different or same base stations called Nodei and Node j

As Node i moving to some indefinite direction, there can be the requirement of hand over. Now the following steps are performed.

Find the capacity of each base station. For this we need to calculate the number of OFDM (Orthogonal Frequency Division Multiplexing) symbols and the overhead symbols in WiMAX MAC frame.

. In this proposed work we defined the triffering on the basis of effective Capacity of the base Stations. Let we have N of base Stations that are the eligible to perform the handover and to take charge of the mobile node. In this case we will find the effective capacity of each node called C1,C2,C3….Cn l base stations BS1, BS2…BSn.

Now we have to elect the base station such that

Min(C(i)) where i>=1 and i<=n

B. *Secure Handover*

The proposed algorithm we will use for make the password based authentication between the two wireless nodes using the public key cryptographic technique. In this algorithm we follow the following steps that helps in makes the password based authentication between two nodes.

Algorithm (Si, Di)

Si and Di are the Mobile Station

Si refers to source node. Di refers to destination node.

Step 1: Request sends by Si to its Base Station B1

Step 2: The Base Station will look the path for the Destination Node Base Station. It will perform the Routing between source and the destination base station

Step 3: Data will be transferred from the Efficient Shortest path

Step 4: On the Receiver side Public key & private key

Step 5: Send public to Si

Step 6: Base Station will perform the Secure Key Exchange between Nodes

Step 7: The public key arrived at Source Node Si

Step 8: Encode the packet of source Si by using public key (key pu).

Step 9: Send the encoded packet to the destination side.

Step 10: On the receiver side.

Step 11: Decode the encrypted packet by help of the private key on destination side.

Step 12: Exit.

IV. NETWORK SIMULATOR

It is used to support networking research and education like Protocol design, traffic studies, etc. Protocol comparison, new architecture designs are also supported. It is used to provide collaborative environment and also Increase confidence in result. Using this technique we do implementation on the basis of their security issues through encryption and decryption algorithms.

We have to set some parameters to provide communication between two nodes.

TABLE I. SIMULATION PARAMETERS

S.No.	PARAMETER	VALUE
1	Frequency Band	5 MHz OFDM
2	Modulation Scheme	1/2 BPSK
3	No of BS	5
4	No of MS	50
5	No of active MS under each BS	5
6	Simulation duration	20 s
7	Requested data rate	50 kbps
8	BS coverage	1000 m
9	Frame duration	20 ms
10	Sampling factor	144/125
11	Propagation model	Two ray ground
12	Antenna Model	Omni directional
13	MS Speed	20 m/s

To perform the complete work we have taken a sample scenario in NS2 with 5 clusters and with one base station in each cluster and then perform the transmission between these clusters[5].

As we can see in Fig 3 the wimax scenario is defined with 5 clusters, each having 10 nodes. We have defined separate colors to identify the clusters easily. Each cluster has its base station as well as mobile station. If cluster5 and cluster 4 wants to communicate, they use BS and MS of cluster 3.

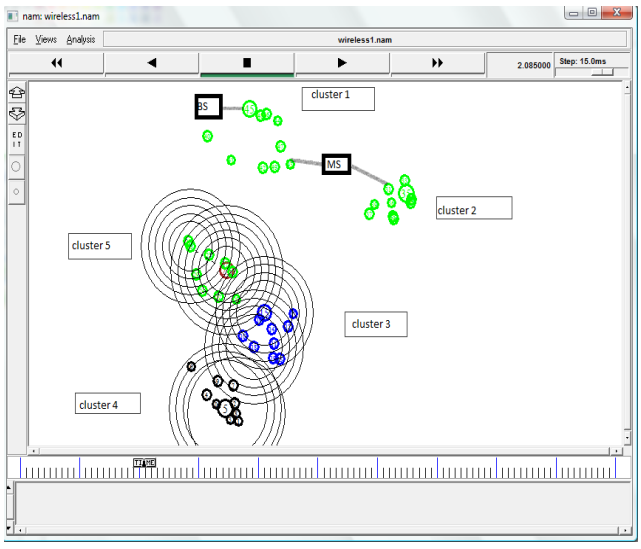

Figure 3. Wimax Communication

V. RESULT

The comparison results between Existing and Proposed Handover is shown by below graphs. In this graph, Dark lines (pink) show the Proposed technology and light lines (yellow) shows the Existing Approach.

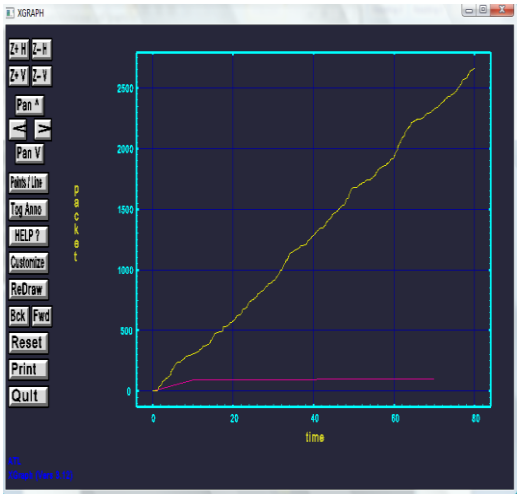

Figure 4. Number of packets transferred

In Fig. 4, the number of packets transferring in Proposed Handover Approach is more as compared with Existing . As time increases WiMAX dark line shows increment in packet transferring.

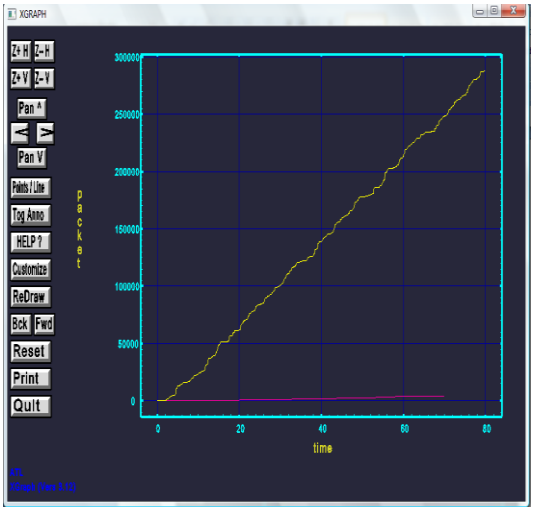

Figure 5. Bit Rate

As in Fig. 5, bit rate is high in Proposed Handover as time increases as compared with Existing Handover. increases as compared with Existing Handover.

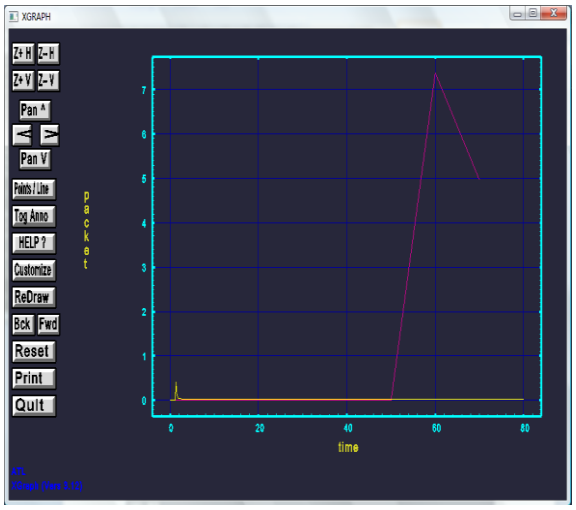

Figure 6. Delay Time

In this Fig. 6, shows that delay time is less in Proposed Handover Approach in fact very constant as compare to Existing .handover Approach

By comparing the result of both techniques shows that the proposed wimax handover technique is more effective and better in data transmission than the other existing communication technique. we attain more number of data per second by running secure and efficient handover.

VI. CONCLUSION

WiMAX network architecture supports all usage models (fixed, mobile & nomadic). It is also support high capacity real time and non real time voice, data and multimedia services while maintaining the appropriate QoS. Moreover it supports idle mode operation and paging for the mobile station. Its network reference model support interoperability. By comparing the secured Handover Approach communication and Existing communication without secure handover and, we observed that Secure Handover Approach offers better services in communication than the Existing Approach. Here we combine three parameters Base Station, Distance and the Transmission Time while performing the handover . By using number of packet in given time , we compare parameter of both technique of communication (with and without secure handover). From which we conclude that by using a secure handover we can increase efficiency of data transfer with reduction of data losses and delays.

ACKNOWLEDGMENT

I am highly thankful to my guide Mr. Arvind Pathak, Assistant Professor, Electronics and Communication Engineering Department of Lingaya's University, Faridabad, for his advice, motivation, guidance, moral support, efforts and the attitude with which he solved all of my queries in making this thesis possible. It has been a great honor to work under him.

I am also thankful to Prof. Pragati Kapoor, Head of Department, Electronics and Communication Engineering Department of Lingaya's University, Faridabad, for providing us with adequate infrastructure in carrying the research work.

REFERENCES

[1] Sen Xu, Chin-Tser Huang, Manton M. Matthews, "Secure Multicast in WiMAX" , Department of Computer Science and Engineering, Univerisity of South Carolina, Columbia, USA.

[2] Sandhya Kulkarni1, H. J. Thontadharya2, J.T. Devaraju, "Performance Evaluation of VoIP in Mobile WiMAX", Simulation and Emulation studies Department of Electronic Science, Bangalore University ,Bangalore, India, 560056.

[3] Shen Gu, Jiajing Wang, "An Enhanced Handover Target Cell Selection Algorithm for WiMAX Network", Department of Electrical Engineering Shanghai Jiao Tong University, *15th Asia-Pacific Conference on Communications (APCC 2009)-184.*

[4] Hrishikesh Venkataraman, Aarthy Krishnamurthy, Poornachand Kalyampudi, Jennifer McManis, Gabriel-Miro Muntean, "Clustered Architecture for Adaptive Multimedia Streaming in WiMAX-based Cellular Networks, World Congress on Engineering and Computer Science 2009 Vol II WCECS 2009, October 20-22, 2009, San Francisco, USA.

[5] Lin SHEN and Xiangquan SHI," A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks", International Journal Of Intelligent Control And Systems, Vol. 13, No. 2, June 2008, 146-151

[6] Analysis of Handover Performance in Mobile WiMAX by Antti Makelainen Helsinki University of Technology.